PRL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/474,203	12/29/1999	YUNZHOU LI	2204/198	1987

2101 7590 12/18/2003

BROMBERG & SUNSTEIN LLP
125 SUMMER STREET
BOSTON, MA 02110-1618

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	6

DATE MAILED: 12/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/474,203	Applicant(s) LI ET AL.	
	Examiner LEYNNA T. HA	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-49 have been examined.

2. Claims 1-8, 15-22, and 26-49 are rejected under 35 U.S.C. 102(b).

3. Claims 9-14, and 23-25 are rejected under 35 U.S.C. 102(e).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. *Claims 1-8, 15-22, and 26-49 are rejected under 35 U.S.C. 102(b) as being anticipated by Mittra (US 5,748,736).*

As per claim 1:

Mittra teaches a method of implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the method comprising:

receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **(col.9, lines 64-65 and col.10, lines 18-20)**

decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic **(col.10, lines 48-50)**

encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and **(col.10, lines 20-21 and lines 45-52)**

forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 2:

Mittra discloses receiving a global key message that identifies the global key. **(col.9, lines 63-65)**

As per claim 3:

Mittra discloses the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 4:

Mittra discloses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. **(col.7, lines 3-14 and col.12, lines 34-37)**

As per claim 5:

Mittra discloses the local key is only available to the given multicast domain. **(col.10, lines 45-52 and col.12, lines 55-59)**

As per claim 6:

Mittra discloses the given multicast domain is a protocol independent multicast domain. **(col.7, lines 1-13)**

As per claim 7:

discloses the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.6, line 39 thru col.7, line 13)**

As per claim 8:

discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone. **(col.6, lines 4-15)**

As per claim 15:

A method of implementing multicast security in a network, the method comprising:

encrypting multicast traffic with a global key, the global key being available to the given multicast domain and one or more multicast domains; **(and col.14, lines 39-42)**

forwarding the global encrypted multicast traffic to the given multicast domain; **(col.9, lines 64-65)**

receiving the global encrypted multicast traffic at the given multicast domain; **(col.10, lines 18-20)**

decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic; **(col.10, lines 48-50)**

encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and **(col.10, lines 20-21 and lines 45-52)**

forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 16:

discloses receiving at the given multicast domain a global key message that identifies the global key. **(col.9, lines 63-65)**

As per claim 17:

discloses the method according to claim 15 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 18:

discloses the method according to claim 15 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. **(col.7, lines 3-14 and col.12, lines 34-37)**

As per claim 19:

discloses the method according to claim 15 wherein the local key is only available to the given multicast domain. **(col.10, lines 45-52 and col.12, lines 55-59)**

As per claim 20:

discloses the method according to claim 15 wherein the given multicast domain is a protocol independent multicast domain. **(col.7, lines 1-13)**

As per claim 21:

discloses the method according to claim 15 wherein the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.6, line 39 thru col.7, line 13)**

As per claim 22:

discusses the method according to claim 15 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

(col.6, lines 4-15)

As per claim 26:

an apparatus for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the apparatus comprising:

a receiver for receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **(col.9, lines 64-65 and col.10, lines 18-20)**

a decryptor for decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic **(col.10, lines 48-50)**

an encryptor for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and **(col.10, lines 20-21 and lines 45-52)**

a traffic forwarder for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 27:

discloses a second receiver for receiving a global key message that identifies the global key. **(col.9, lines 63-65)**

As per claim 28:

discloses the apparatus according to claim 26 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 29:

discloses the apparatus according to claim 26 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. **(col.7, lines 3-14 and col.12, lines 34-37)**

As per claim 30:

discloses the apparatus according to claim 26 wherein the local key is only available to the given multicast domain. **(col.10, lines 45-52 and col.12, lines 55-59)**

As per claim 31:

discloses the apparatus according to claim 26 wherein the given multicast domain is a protocol independent multicast domain. **(col.7, lines 1-13)**

As per claim 32:

discloses the apparatus according to claim 26 wherein the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.6, line 39 thru col.7, line 13)**

As per claim 33:

discusses the method according to claim 26 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

(col.6, lines 4-15)

As per claim 34:

teaches A computer program product for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the computer comprising:

program code for receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **(col.9, lines 64-65 and col.10, lines 18-20)**

program code for decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic **(col.10, lines 48-50)**

program code for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and **(col.10, lines 20-21 and lines 45-52)**

program code for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 35:

discloses a program code for receiving a global key message that identifies the global key. **(col.9, lines 63-65)**

As per claim 36:

discloses the computer program code according to claim 34 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 37:

discloses the computer program code according to claim 34 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. **(col.7, lines 3-14 and col.12, lines 34-37)**

As per claim 38:

discloses the computer program code according to claim 34 wherein the local key is only available to the given multicast domain. **(col.10, lines 45-52 and col.12, lines 55-59)**

As per claim 39:

discloses the computer program code according to claim 34 wherein the given multicast domain is a protocol independent multicast domain.

(col.7, lines 1-13)

As per claim 40:

discloses the computer program code according to claim 34 wherein the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.6, line 39 thru col.7, line 13)**

As per claim 41:

discusses the computer program code according to claim 34 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone. **(col.6, lines 4-15)**

As per claim 42:

teaches an apparatus of implementing multicast security in a network, the apparatus comprising:

means for encrypting multicast traffic with a global key, the global key being available to the given multicast domain and one or more multicast domains; **(col.9, lines 64-65 and col.10, lines 18-20)**

means for forwarding the global encrypted multicast traffic to the given multicast domain; **(col.10, lines 15-19)**

means for receiving the global encrypted multicast traffic at the given multicast domain; **(col.13, lines 4-7)**

means for decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic; **(col.10, lines 48-50)**

means for encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and

(col.10, lines 20-21 and lines 45-52)

means for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 43:

discloses means for receiving at the given multicast domain a global key message that identifies the global key. **(col.9, lines 63-65)**

As per claim 44:

discloses the apparatus according to claim 42 wherein the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 45:

discloses the apparatus according to claim 42 wherein the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message. **(col.7, lines 3-14 and col.12, lines 34-37)**

As per claim 46:

discloses the apparatus according to claim 42 wherein the local key is only available to the given multicast domain. **(col.10, lines 45-52 and col.12, lines 55-59)**

As per claim 47:

discloses the apparatus according to claim 42 wherein the given multicast domain is a protocol independent multicast domain. **(col.7, lines 1-13)**

As per claim 48:

discloses the apparatus according to claim 42 wherein the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.6, line 39 thru col.7, line 13)**

As per claim 49:

discusses the apparatus according to claim 42 wherein the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

(col.6, lines 4-15)

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. *Claims 9-14 and 23-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Haggerty, Et. Al. (US 6,049,878).*

As per claim 9:

Haggerty, Et. Al. teaches a method of implementing multicast security in a given multicast domain, the method comprising:

receiving multicast traffic that is encrypted with a global key, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **(col.23, lines 30-40)**

determining that the given multicast domain contain no network devices interested in the received multicast traffic; and **(col.31, lines 35-40)**

sending a terminate message to no longer forward the received multicast traffic to the give multicast domain. **(col.31, line 42 thru col.32, line 15)**

As per claim 10:

Haggerty discloses receiving a global key message that identifies the global key. **(col.23, lines 30-40)**

As per claim 11:

Haggerty teaches a method according to claim 9, further comprising:

determining, after having sent the terminate message, that the given multicast domain contains one or more network devices interested in the received multicast traffic; and **(col.29, lines 50-52)**

sending a resume message to once again forward the received multicast traffic to the given multicast domain. **(col.29, lines 52-54)**

As per claim 12:

Haggerty discusses the given multicast domain is a protocol independent multicast domain. **(col.14, lines 28-52)**

As per claim 13:

Haggerty discloses the given multicast domain is a group of contiguous protocol independent multicast domains. **(col.14, lines 28-52)**

As per claim 14:

Haggerty discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone. **(col.11, lines 38-63)**

As per claim 23:

Haggerty teaches a method of implementing multicast security in a given multicast domain, the method comprising:

receiving multicast traffic; **(col.29, lines 20-25)**

constructing, in response to the received multicast traffic, an information message that alerts other multicast domains of the security capabilities of the give multicast domain; and **(col.29, lines 25-26)**

forwarding the information message to at least one other multicast domain. **(col.29, lines 27-32)**

As per claim 24:

Haggerty discloses the information message is a part of a multicast protocol message. **(col.14, lines 28-52)**

As per claim 25:

Haggerty discusses one or more bits in one or more fields of the multicast message are set to alert other multicast domains of the security capabilities of the give multicast domain; and **(col.29, lines 20-32)**

Conclusion

For further details for the cited rejection above, please refer to:

Mittra: col.4, line 6...ET. Seq.

Haggerty, Et. Al: col.7, line 24...ET. Seq.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

LHa

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100